DHS Control Systems Security Program

www.inl.gov

Cyber researchers Ken Rohde and Jonathan Chugg review control system configurations during a training exercise.

We're all connected. We're all online. Tied to one another like never before, our computers, smart phones, and social networks provide us with a vast ability to communicate and share information. But massive interconnection has its risks. When basic needs like power, water, and emergency services can be disrupted by a cyber virus or deliberate hack, utilities and other critical infrastructures face a dilemma that must be solved.

In the U.S., most of the nation's 18 critical infrastructure sectors have transitioned from operating in an isolated analog environment to one of interconnected digital command and control. Today, service providers rely on control systems to manage the flow of water at dams, open breakers on power grids, and provide real-time operational feedback. As technology has rapidly evolved, cybersecurity has transitioned from an afterthought to a leading movement. Now, government, private industry, and academia are working together to reduce cyber risks.

To broadly coordinate cyber and control systems security efforts, the Department of Homeland Security's National Cyber Security Division established the Control Systems Security Program (CSSP). The CSSP aids industry by developing mitigation tools, conducting hands-on training, providing rapid cyber response and analysis, and increasing awareness through working groups and forums. The program's efforts are guided by the National Infrastructure Protection Plan and the Strategy to Secure Control Systems.

Since 2004, the CSSP has provided immersive training to thousands of infrastructure owners and operators, and led information-sharing sessions at events like the Industrial Control Systems Joint Working Group. The program's tools include the Control Systems Evaluation Tool (CSET) and the Procurement Language for Control Systems.

Quick Facts

- The DHS Control Systems Analysis Center is managed by cyber and infrastructure experts from Idaho National Laboratory.
- The Procurement Language for Control Systems helps owners and operators specify the right security products for their specific needs.
- The CSET tool passively alerts control systems operators to system vulnerabilities, misconfigurations, and potential solutions.
- The Industrial Control Systems Cyber Emergency Response Team can rapidly analyze and respond to suspicious control system incidents.

For More Information

Marty Edwards
INL Program Manager
(208) 526-9372
marty.edwards@inl.gov

For Program Information
1-877-776-7585
cssp@dhs.gov
www.us-cert/control_systems

Idaho National Laboratory

09-50787 R6-11